Virginia Information Technologies Agency

Commonwealth Information Security Council
Risk Management Committee Meeting

April 26, 2010
3:30-4:30 pm CESC

Risk Management Committee members attending:

Goran Gustavsson, Co-Chair *
Ed Miller, Co-Chair *
Aaron Mathes, OAG, Co-Chair *
Ross McDonald, DSS *
Joshua Cole, Dept of Aviation *
Jack Spooner, DOA *
Jeremy Greenwood, TRS *

* (Teleconference to CESC)

Risk Management Committee members absent:

Bob Auton, DJJ

Also Attending:

John Green, COV CISO
Benny Ambler, CSRM
Mauri Shaw, CRSM

Topic: Risk Management - Discussion of new Code Requirement (COV risk management program – 2.2-2009, Additional duties of the CIO relating to security of government information, Section H.

- the April 19, 2010 Risk Management meeting was re-scheduled due to John Green not able to be present - members were asked to schedule a teleconference (4/26/2010) to help address and explain and receive feedback about the new legislation to add a risk management program to the CIO duties – ref. " 2.2-2009, Additional duties of the CIO relating to security of government information,

  H. The CIO shall also develop policies, procedures, and standards that shall address the creation and operation of a risk management program designed to identify information technology security gaps and develop plans to mitigate the gaps. All agencies in the Commonwealth shall cooperate with the CIO. Such cooperation includes, but is not limited to, (i) providing the CIO with information required to create and implement a Commonwealth risk management program; (ii) creating an agency risk management program; and (iii) complying with all other risk management activities.

Teleconference Discussion points for establishing procedures to fulfill the Code requirement:

- Risk management data could be collected by the ISO's (possibly collected on a simple template to start.

- Determine whether using NIST complements the COV Risk Management Program?
- Is their another "Risk Management" framework to use other than NIST?
- Can the ISO's and CSRM work their way towards a new compliance effort over time?
- Need strategic vision collected through questionnaires.
- Possibly have a Risk Management Officer per agency?
- Possibly separating Risk Management from SEC501 and creating a whole separate requirement for Risk Management?
- Create a Risk Profile packet of Information (e.g. "Open issues")
- Need a clear statement of what we (RM Committee and CSRM) hope to get out of this new requirement.
- Can expect push back from agencies possibly: (e.g. agency feels information is private on risk assessment, or agency ISO fears more work on his behalf, or more cost, etc.)
- Need to identify "IT Security Gaps" and resultant mitigation procedures/measures resolution as being part of an "economies of scale" opportunity - the more agencies needing to close the "IT Security Gap" the more probability of funding being obtained.
- It may be possible to "detach" the sensitive system information shared from the "vulnerabilities reported" to lessen the sensitive system information that is expected to be shared.

Going forward with action plan:

- Several to review RSAM product and report back on its capabilities.
- Possibly the RSAM (type of product) would offer up support for BIA, COOP and DR and open up other funding streams?